digital signature

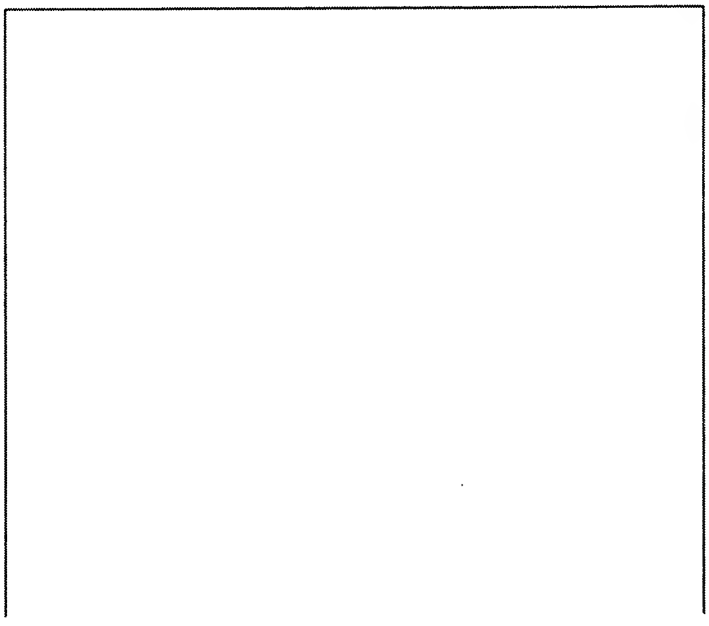
Also found in: Wikipedia, Hutchinson

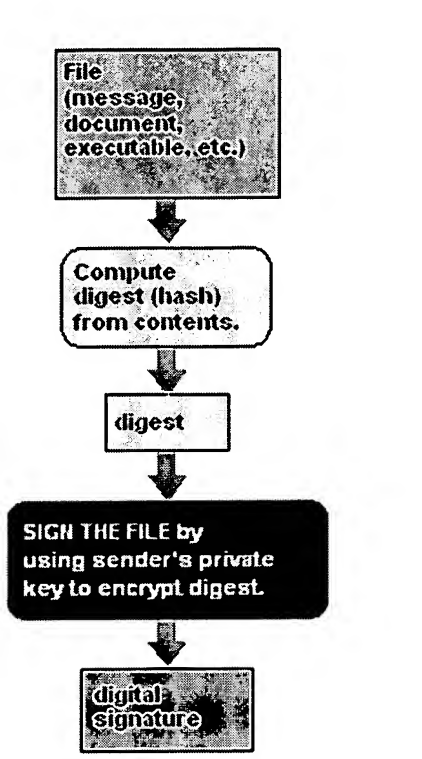
0.01 sec.

A digital guarantee that information has not been modified, as if it were protected by a tamper-proof seal that is broken if the content were altered. The two major applications of digital signatures are for setting up a secure connection to a Web site and verifying the integrity of files transmitted (more below).

An Encrypted Digest

The digital signature is an encrypted digest of the file (message, document, driver, program) being signed. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 (see MD5 and SHA-1) and then encrypted with the private part of a public/private key pair (see RSA). To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker. See MD5.





An Encrypted Digest

A digital signature is an encrypted digest of a file. The digest was created with a one-way hash function from the file's contents.

Signed Certificates

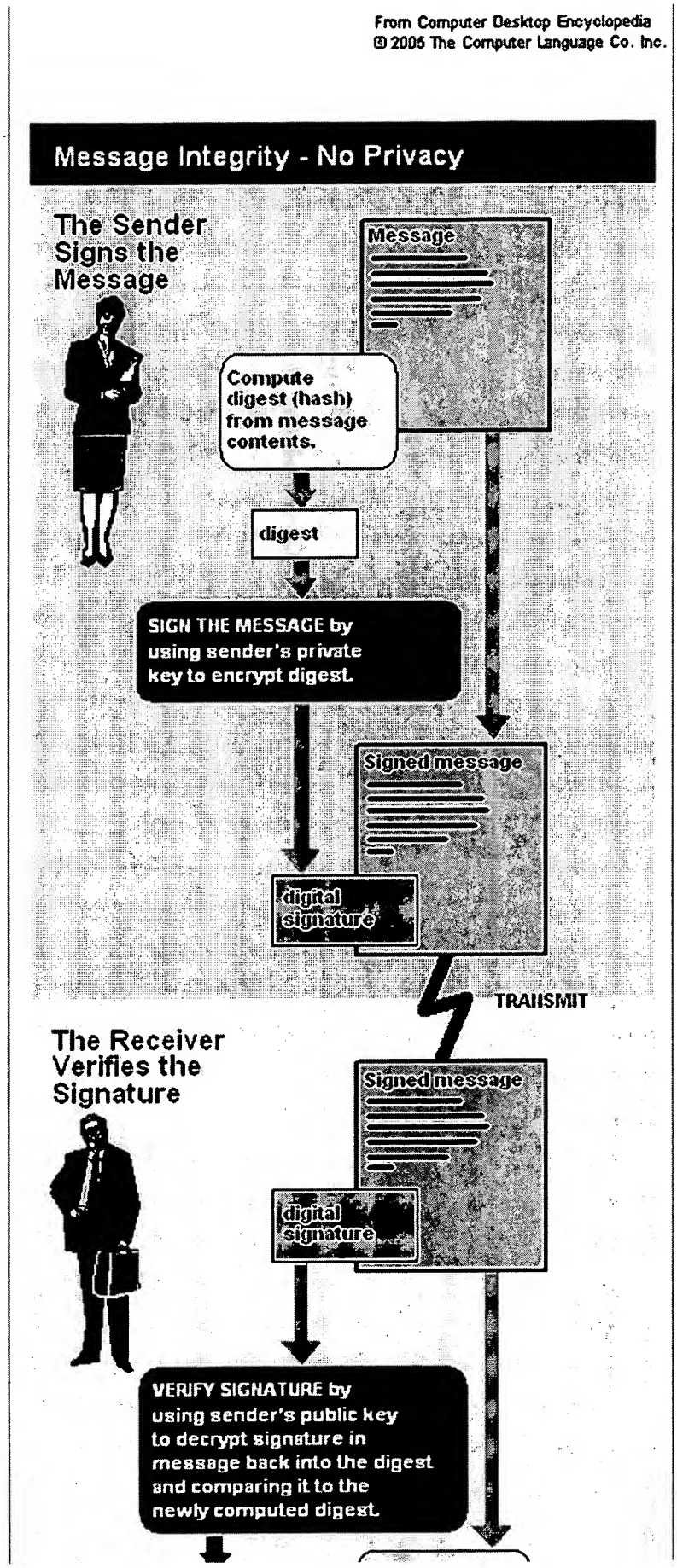
The first major application for digital signatures is digital certificates. "Signed" digital certificates are used to verify the identity of an organization or individual. They are widely used to authenticate a Web site in order to establish an encrypted connection for credit card and other confidential data (see SSL and digital certificate).

Signed Files

The second major application for digital signatures is "code signing," which verifies the integrity of executable files downloaded from a Web site. Code signing also uses signed digital certificates to verify the identity of the site (see code signing and digital certificate). Also see digital envelope and electronic signature.

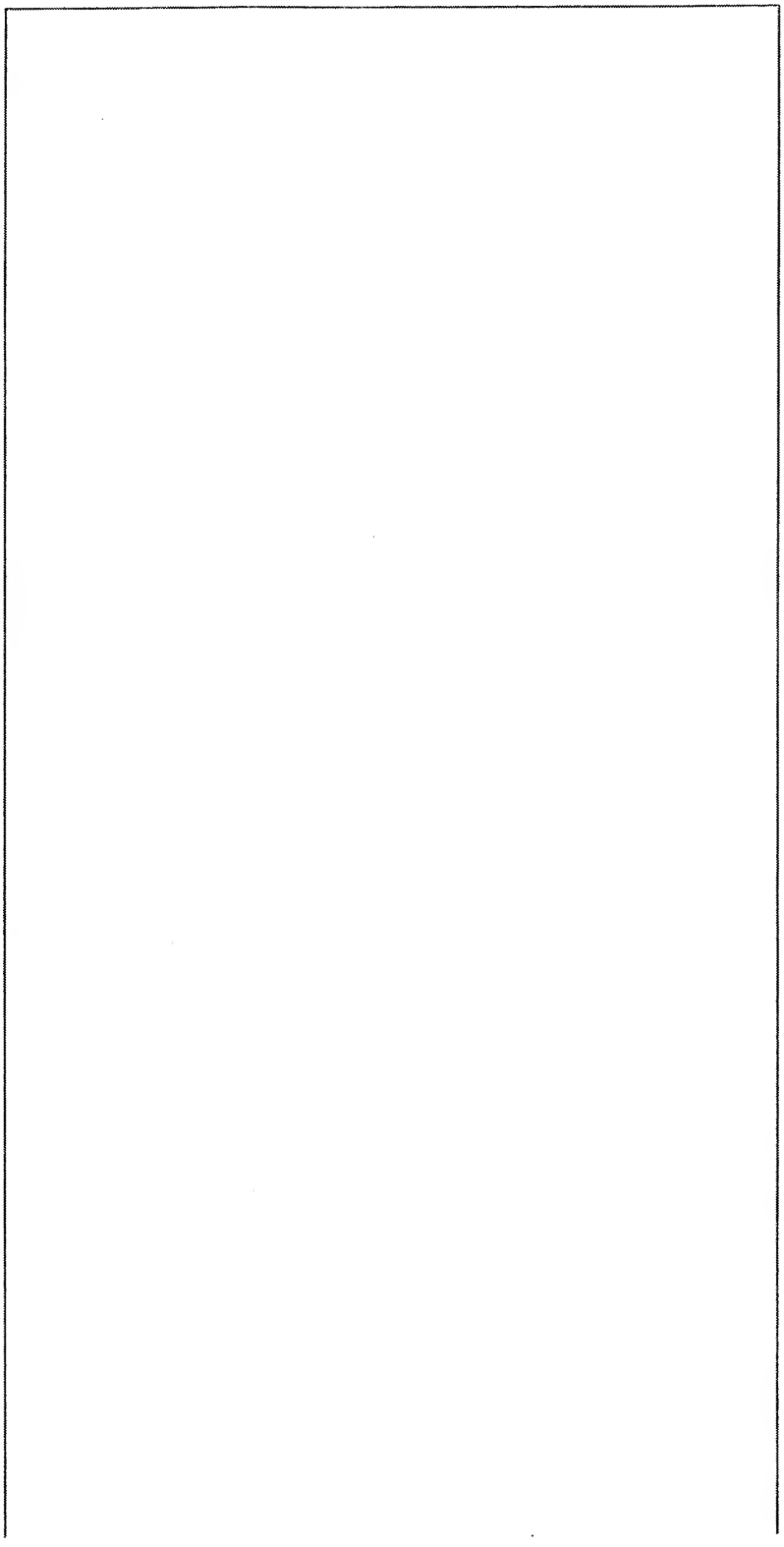
The Illustrations Below

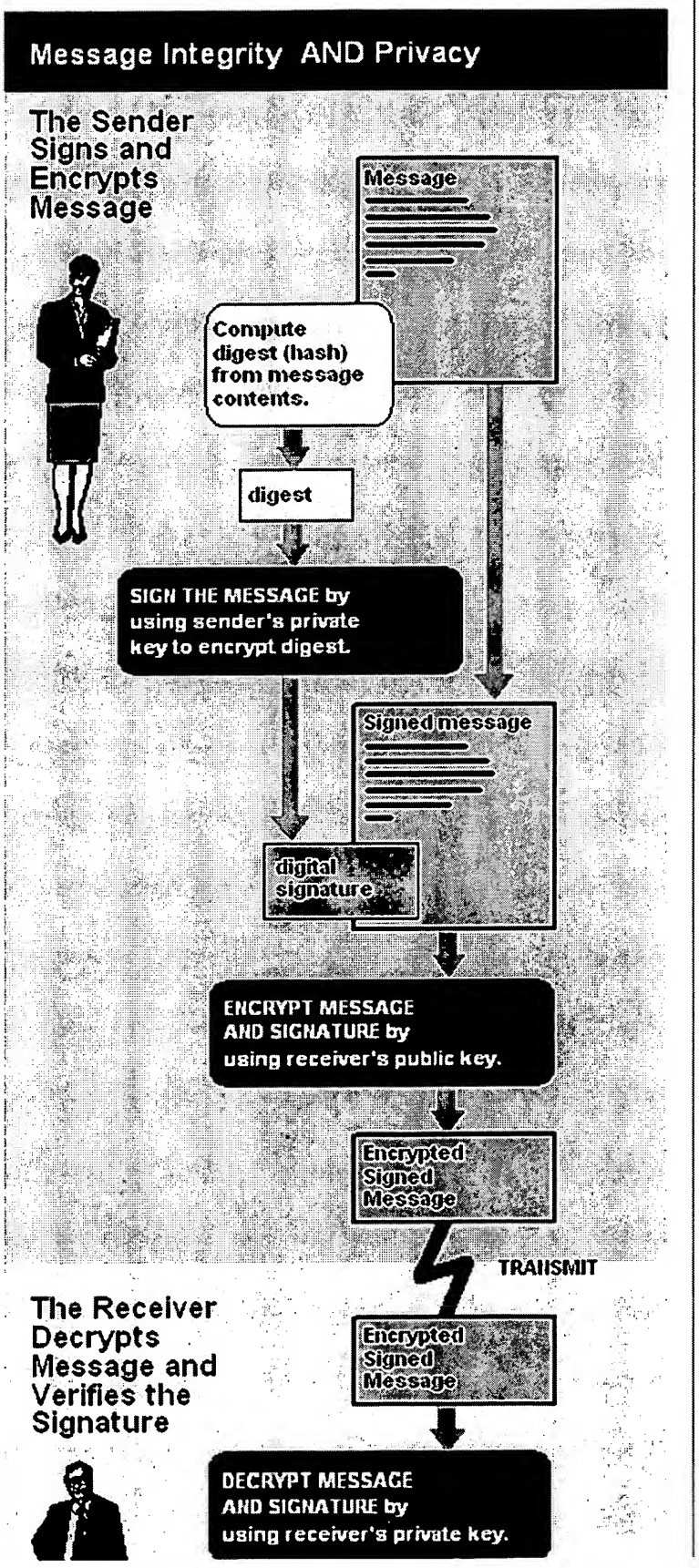
The following two illustrations show how digital signatures are used for data integrity in both non-private and private exchanges. Because of the requirement of disseminating keys, the following methods are used mostly between two parties that communicate with each other on a regular basis and not by the public in general. The references to the man and woman are used to help explain the concept; however, all functions are automatically performed by the software.



Integrity, But No Privacy

The woman makes her message tamper proof by encrypting the digest into a "digital signature," which accompanies the message. At the receiving side, the man uses her public key to verify the signature. However, the message text is sent "in the clear" and could be read by an eavesdropper.





Message Integrity and Privacy

In this example, the woman signs her message and also encrypts the signature and message with the man's public key for privacy (confidentiality). When he receives the encrypted signed message, he decrypts it with his private key to expose the text he can now read along with the signature. He then verifies the signature to ensure the message was not tampered with.

Mentioned in

CIA
digital certificate
digitally signed
DNSSec
e-mail authentication
ECC
El Gamal algorithm
electronic signature
GNU Privacy Guard
hash function
HSM
JCA
MD5
message digest
nonrepudiation
NSBD
one-way hash function
PEM
PKCS

More results ▸▸

Computing browser

digital resolution
digital rights management
digital satellite radio
digital service unit
digital signal
Digital Signal Processing
Digital Signal Processing Language
digital signature
Digital Signature Standard
digital signatures
Digital Simulation Language
Digital Simultaneous Voice and Data
digital single lens reflex
DIGITAL Standard MUMPS
Digital Subscriber Line

Full browser

■ Digital signal processing
● Digital Signal Processing Hardware
● Digital Signal Processing Laboratory
● Digital Signal Processing Language
● Digital Signal Processing Language
● Digital Signal Processing Power Supply
● Digital signal processor
Digital signal processor
■ Digital signal processor
● Digital Signal Processor for Space and Automotive Application Pilot
● Digital Signal Processor Resource Manager
Digital signal processors
■ Digital signal processors
● Digital Signal Protocol
● Digital Signal Synchronization (Sprint)
● Digital Signal, Level 0 (64 Kb/s data/voice channel)
● Digital Signal, Level 1 (1.544 Mbit/s T1 Interface; DS0 x 24 mux)
● Digital Signal, Level 2 (6.176 Mbit/s, DS1 x 4 mux)
● Digital Signaling Rate
● Digital Signaling Unit
● Digital signals
■ Digital signals
Digital signals processor
■ Digital signals processor
digital signature
● Digital Signature Algorithm
● Digital Signature Algorithm
■ Digital Signature Algorithm
● Digital Signature Initiative
● Digital Signature Layer (email encryption)
● Digital Signature Messaging System (digital certificate system)
● Digital Signature Pilot Project
● Digital Signature Standard
● Digital Signature Standard
■ Digital Signature Standard
■ Digital Signature Transponder
● Digital Signature Trust (Zion Bankcorporation)
● Digital Signature Trust Company
● Digital signatures
Digital signatures
■ Digital signatures
● Digital Simple Data Interface
● Digital Simple Data Interface Enhanced
● Digital Simulation Facility
● Digital Simulation Language
● Digital Simulation Test Equipment
● Digital Simultaneous Voice and Data
● Digital Simultaneous Voice and Data
● Digital Simultaneous Voice Over Data